(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 998 542 A1**

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
18.05.2022 Bulletin 2022/20

(21) Application number: **20836615.3**

(22) Date of filing: **05.03.2020**

(51) International Patent Classification (IPC):
G06F 21/31 *(2013.01)* ***G06F 21/44*** *(2013.01)*
G06F 21/45 *(2013.01)* ***G06F 21/60*** *(2013.01)*
H04L 12/28 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G06F 21/31; G06F 21/44; G06F 21/45; G06F 21/60; H04L 12/28

(86) International application number:
PCT/JP2020/009376

(87) International publication number:
WO 2021/005831 (14.01.2021 Gazette 2021/02)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **08.07.2019 JP 2019126824**

(71) Applicant: **OMRON Corporation**
Shiokoji-dori, Shimogyo-Ku
Kyoto-shi
Kyoto 600-8530 (JP)

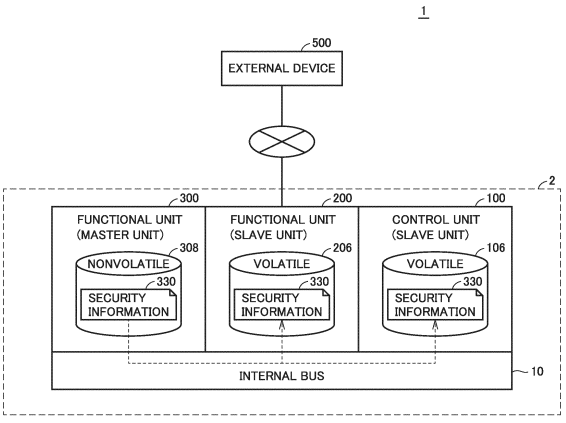
(72) Inventors:
- **NISHIYAMA, Yoshihide**
  Kyoto-shi, Kyoto 600-8530 (JP)
- **NAGATA, Yuta**
  Kyoto-shi, Kyoto 600-8530 (JP)

(74) Representative: **Mewburn Ellis LLP**
Aurora Building
Counterslip
Bristol BS1 6BX (GB)

(54) **CONTROL SYSTEM AND CONTROL METHOD**

(57) Provided is a technique for centrally managing security information in a control system (2) including a plurality of units. Control system (2) includes a master unit (300) connected to a bus (10) and a slave unit (200) connected to bus (10) and communicating with master unit (300) via bus (10). Master unit (300) includes a non-volatile memory (308) that stores first security information (330) as information to be concealed. Slave unit (200) includes a volatile memory (206). Slave unit (200) receives first security information (330) from master unit (300) at a predetermined timing, and stores first security information (330) in volatile memory (206).

FIG.1



EP 3 998 542 A1

Description

TECHNICAL FIELD

[0001] The present disclosure relates to a technique for managing security information in a control system including a plurality of units.

BACKGROUND ART

[0002] At production sites using factory automation (FA), control units such as programmable logic controllers (PLCs) are used to control various devices. In recent years, control units that are connectable to external devices have become widespread. Regarding such a control unit, PTL 1 (Japanese Patent Laying-Open No. 2016-194808) discloses a PLC configured to access a database of an external device.

CITATION LIST

PATENT LITERATURE

[0003] PTL 1: Japanese Patent Laying-Open No. 2016-194808

SUMMARY OF INVENTION

TECHNICAL PROBLEM

[0004] Various functional units may be connected to the control unit. Various applications can be installed in each functional unit. Users can add functional units and install applications as needed.

[0005] Each functional unit is independent of other functional units, and it is necessary to manage information such as account information and digital certificates (hereinafter, also referred to as "security information") for each functional unit. Thus, with an increasing number of functional units, the user may set an easy password or forget the password, and management of security information becomes complicated. Therefore, a technique for centrally managing security information in a control system including a plurality of units is desired.

SOLUTION TO PROBLEM

[0006] In one example of the present disclosure, a control system including a plurality of units is provided. The plurality of units includes a master unit connected to a bus and a slave unit connected to the bus and communicating with the master unit via the bus. The master unit has a nonvolatile memory that stores first security information as information to be concealed. The slave unit has a volatile memory. The slave unit receives the first security information from the master unit at a predetermined timing and stores the first security information in the volatile memory.

[0007] In the present disclosure, the slave unit stores security information received from the master unit in the volatile memory. As a result, the security information disappears from the master unit each time power supply to the control system is stopped. On the other hand, security information stored in the nonvolatile memory of the master unit does not disappear even when the power supply to the control system is stopped. As a result, the security information can be centrally managed.

[0008] In one example of the present disclosure, the predetermined timing includes a timing at which power of the control system is turned on.

[0009] In the present disclosure, the slave unit receives security information from the master unit each time the power of the control system is turned on, and thus the security information can be kept updated.

[0010] In one example of the present disclosure, the first security information includes account information of a user. In response to reception of a request for data access to the slave unit from an external device configured to be communicable with the slave unit, the slave unit requests the external device to input account information, and in a case where the account information input to the external device is registered in the first security information stored in the volatile memory, the slave unit allows data access to the slave unit by the external device.

[0011] In the present disclosure, the slave unit can authenticate the user on the basis of the account information received from the master unit.

[0012] In one example of the disclosure, the first security information includes a digital certificate. The first security information includes a digital certificate, and in response to reception of a request for acquisition of data stored in the slave unit from the external device configured to be communicable with the slave unit, the slave unit sends the digital certificate stored in the volatile memory to the external device.

[0013] In the present disclosure, the slave unit can communicate with the external device on the basis of the digital certificate received from the master unit.

[0014] In one example of the present disclosure, the slave unit further includes a nonvolatile memory that stores second security information as information to be concealed. In a case where there is conflicting information between information included in the first security information and information included in the second security information, the slave unit determines which of the conflicting information to prioritize in accordance with a predetermined rule.

[0015] The present disclosure resolves information conflict between the first security information and the second security information.

[0016] In one example of the present disclosure, the master unit receives the second security information from the slave unit at the predetermined timing and stores the second security information in the volatile memory of the master unit.

[0017] In the present disclosure, the security information can be distributed to the master unit and the slave unit and managed.

[0018] In one example of the present disclosure, the slave unit includes a control unit that controls a drive device.

[0019] In the present disclosure, the security information used in the control unit can be centrally managed by the master unit.

[0020] Another example of the present disclosure provides a control method of a control system including a plurality of units. The plurality of units includes a master unit connected to a bus and a slave unit connected to the bus and communicating with the master unit via the bus. The control method includes storing, by the master unit, first security information as information to be concealed in a nonvolatile memory of the master unit, receiving, by the slave unit, the first security information from the master unit at a predetermined timing, and storing, by the slave unit, the first security information received from the master unit in a volatile memory of the slave unit.

[0021] In the present disclosure, the slave unit stores security information received from the master unit in the volatile memory. As a result, the security information disappears from the master unit each time power supply to the control system is stopped. On the other hand, in the master unit, security information stored in the nonvolatile memory of the master unit does not disappear even when the power supply to the control system is stopped. As a result, the security information can be centrally managed.

BRIEF DESCRIPTION OF DRAWINGS

[0022]

Fig. 1 is a diagram illustrating a configuration example of an information processing system according to an embodiment.

Fig. 2 is an external view illustrating a configuration example of a control system according to the embodiment.

Fig. 3 is a schematic diagram illustrating a hardware configuration example of a control unit constituting the control system according to the embodiment.

Fig. 4 is a schematic diagram illustrating a hardware configuration example of a functional unit constituting the control system according to the embodiment.

Fig. 5 is a schematic diagram illustrating a hardware configuration example of a functional unit constituting the control system according to the embodiment.

Fig. 6 is a schematic diagram illustrating a hardware configuration example of an external device constituting the information processing system according to the embodiment.

Fig. 7 is a diagram illustrating an example of a unit configuration of the information processing system according to the embodiment.

Fig. 8 is a diagram illustrating a data flow between the functional unit, the functional unit, and the external device.

Fig. 9 is a diagram illustrating an example of a screen displayed on the external device according to the embodiment.

Fig. 10 is a diagram of registered account information included in security information.

Fig. 11 is a diagram illustrating a configuration example of a control system according to a first modification.

Fig. 12 is a diagram illustrating a process of merging the security information.

Fig. 13 is a diagram illustrating a configuration example of a control system according to a second modification.

Fig. 14 is a diagram illustrating a configuration example of a control system according to a third modification.

Fig. 15 is a diagram of key information included in the security information.

DESCRIPTION OF EMBODIMENTS

[0023] Hereinafter, an embodiment of the present invention will be described with reference to the drawings. In the following description, the same parts and elements are designated by the same reference signs. Names and functions of such parts and elements are the same. Therefore, the detailed description of the parts and elements will not be repeated.

<A. Application example>

[0024] An application example of the present invention will be described with reference to Fig. 1. Fig. 1 is a diagram illustrating a configuration example of an information processing system 1 according to the embodiment.

[0025] Information processing system 1 includes one or more control systems 2 and one or more external devices 500. Control system 2 is an FA system that automates a production process. Control system 2 includes a control unit 100 and functional units 200 and 300. Functional unit 300 functions as a master unit. Control unit 100 and functional unit 200 function as slave units. A master-slave relationship is set in advance.

[0026] Functional unit 200 and external device 500 are connected to an external network. Communication between functional unit 200 and external device 500 is achieved by Ethernet (registered trademark). External device 500 is, for example, a laptop or desktop personal computer (PC), a tablet terminal, a smartphone, a human machine interface (HMI), or another information processing terminal.

[0027] Control unit 100, functional unit 200, and functional unit 300 are connected to each other by an internal bus 10. These units communicate with each other via internal bus 10.

[0028] Control unit 100 is, for example, a PLC. Control unit 100 controls a drive device (not shown) in accordance with a user program designed in advance. The drive device includes various industrial devices that automate the production process. Examples of the drive device include a robot controller, a servo driver, an arm robot controlled by the robot controller, a servo motor controlled by the servo driver, and the like. Further, the drive device may include a visual sensor for photographing working, other devices used in the production process, and the like.

[0029] Control unit 100 has a volatile memory 106. Volatile memory 106 is a general term for a memory in which stored information is erased when power supply stops. Volatile memory 106 is, for example, a random access memory (RAM) such as static random access memory (SRAM) or dynamic random access memory (DRAM).

[0030] Functional unit 200 is connected to control unit 100. Various applications for providing various services related to control system 2 may be installed in functional unit 200. Functional unit 200 has a volatile memory 206. Volatile memory 206 is, for example, RAM such as SRAM or DRAM

[0031] Functional unit 300 is a unit that centrally manages security information 330 as information to be concealed. Functional unit 300 is, for example, a security guard unit (SGU). Security information 330 includes, for example, account information and digital certificates used by various units. Security information 330 is stored in a nonvolatile memory 308 of functional unit 300.

[0032] Nonvolatile memory 308 is a general term for memory that can continue to hold information without any power supply. Nonvolatile memory 308 is, for example, a read only memory (ROM), a hard disk, or a flash memory.

[0033] Functional unit 300 as a master unit sends security information 330 to control unit 100 and functional unit 200 as the slave units at a predetermined timing. Control unit 100 stores security information 330 received from functional unit 300 in volatile memory 106. Similarly, functional unit 200 stores security information 330 received from functional unit 300 in volatile memory 206.

[0034] The timing at which security information 330 is distributed is not limited. In a certain aspect, security information 330 is distributed to the slave units at a timing when power of control system 2 is turned on. In another aspect, security information 330 is distributed to the slave units at predetermined intervals. In still another aspect, security information 330 is distributed to the slave units at a timing of receiving an acquisition instruction or update instruction by a user operation.

[0035] As described above, control system 2 has functional unit 300 that centrally manages the security information. This eliminates the need for a user to manage the account information, digital certificates, and the like for each unit, and eliminates complexity of managing the security information. As a result, security holes caused by incorrect or old settings can be prevented. Further, when security information 330 is managed in one place, there will be less places to be confirmed when an abnormality occurs, and the abnormality can be dealt with promptly.

[0036] Furthermore, the security information is distributed via internal bus 10, and there is no need to connect to the external network. This reduces possibility that the security information is leaked to outside and improves a security level of control system 2.

[0037] Security information 330 is stored in volatile memories 106 and 206. Thus, security information 330 does not remain on the slave units after the power of control system 2 is cut off. On the other hand, security information 330 stored in nonvolatile memory 308 of functional unit 300 does not disappear even when the power supply to control system 2 is stopped. As a result, security information 330 is not duplicated, and security information 330 is centrally managed more reliably.

[0038] Further, when security information 330 is centrally managed, the user does not need to take measures against information leakage for all the units. That is, the user can improve the security level by taking measures against information leakage intensively for nonvolatile memory 308 of functional unit 300. For example, when a memory with an encryption function is used for nonvolatile memory 308, a leakage risk of security information 330 can be reduced. Further, since the user only needs to take measures against information leakage only for nonvolatile memory 308, costs can be suppressed.

<B. Control system 2>

[0039] Control system 2 illustrated in Fig. 1 will be described with reference to Fig. 2. Fig. 2 is an external view illustrating a configuration example of control system 2.

[0040] With reference to Fig. 2, control system 2 includes one or more control units 100, one or more functional units 200, one or more functional units 300, one or more functional units 400, and a power supply unit 450.

[0041] Control unit 100 and functional unit 200 are connected to each other via an arbitrary data transmission line. Control unit 100, functional unit 200, and one or more functional units 300 and 400 are connected to each other via internal bus 10 (see Fig. 1).

[0042] Control unit 100 executes central processing in control system 2. Control unit 100 executes a control calculation for controlling a controlled object according to an arbitrarily designed requirement specification. In the configuration example illustrated in Fig. 2, control unit 100 has one or more communication ports. Control unit 100 corresponds to a processing execution unit that executes standard control in accordance with a standard control program.

[0043] Functional unit 200 is connected to control unit 100 and is charge of a communication function with other devices. In the configuration example illustrated in Fig. 2, functional unit 200 has one or more communication ports.

[0044] Functional unit 300 is an optional unit and is connected to control unit 100 as needed. Functional unit 300 may typically include a security guard unit (SGU), a communication unit having a data exchange function by object linking and embedding for process control unified architecture (OPC UA), an artificial intelligence (AI) unit having a preventive maintenance function by AI, and the like.

[0045] Functional unit 400 provides various functions for achieving control for various control targets by control system 2. Functional unit 400 may typically include an I/O unit, a safety I/O unit, a communication unit, a motion controller unit, a temperature control unit, a pulse counter unit, and the like. Examples of the I/O unit include a digital input (DI) unit, a digital output (DO) unit, an analog input (AI) unit, an analog output (AO) unit, a pulse catch input unit, and a composite unit having a mixture of a plurality of types. The safety I/O unit is in charge of I/O processing related to safety control.

[0046] Power supply unit 450 supplies power of a predetermined voltage to each unit constituting control system 2.

<C. Hardware configuration example of each unit>

[0047] Next, a hardware configuration example of each unit constituting control system 2 according to the present embodiment will be described.

(c1: Control unit 100)

[0048] Fig. 3 is a schematic diagram illustrating a hardware configuration example of control unit 100 constituting control system 2 according to the present embodiment. With reference to Fig. 3, control unit 100 includes, as main components, a processor 102 such as a central processing unit (CPU) or a graphical processing unit (GPU), a chipset 104, a volatile memory 106, nonvolatile memory 108, a communication controller 110, a universal serial bus (USB) controller 112, a memory card interface 114, network controllers 116, 118, and 120, an internal bus controller 122, and an indicator 124.

[0049] Processor 102 reads various programs stored in nonvolatile memory 108, develops the programs in volatile memory 106, and executes the programs to implement control calculation related to standard control and various processing as described later. Chipset 104 mediates a data exchange between processor 102 and each component, and thus implements the processing of control unit 100 as a whole.

[0050] In addition to a system program, nonvolatile memory 108 stores a control program that operates in an execution environment provided by the system program.

[0051] Communication controller 110 is in charge of exchanging data with functional unit 300. As communication controller 110, for example, a communication chip corresponding to an internal bus, Ethernet, or the like can be adopted.

[0052] USB controller 112 is in charge of exchange data with an arbitrary information processing device via USB connection.

[0053] A memory card 115 is attachable to and detachable from memory card interface 114, and memory card interface 114 can write data such as a control program and various settings to memory card 115 or read data such as a control program and various settings from memory card 115.

[0054] Each of network controllers 116, 118, and 120 is in charge of exchanging data with an arbitrary device via the network. Network controllers 116, 118, and 120 may employ an industrial network protocol such as EtherCAT (registered trademark), EtherNet/IP (registered trademark), DeviceNet (registered trademark), or CompoNet (registered trademark).

[0055] Internal bus controller 122 is in charge of exchanging data with functional unit 200, one or more functional units 300, and one or more functional units 400 constituting control system 2. As the internal bus, a communication protocol unique to a manufacturer may be used, or a communication protocol that is the same as or compliant with a protocol of any industrial network may be used.

[0056] Indicator 124 notifies an operating state of control unit 100 and the like and includes one or more LEDs disposed on a surface of the unit.

[0057] Although Fig. 3 illustrates the configuration example in which necessary functions are provided by processor 102 executing the programs, some or all of these provided functions may be implemented by using a dedicated hardware circuit (for example, an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA), or the like. Alternatively, a main part of control unit 100 may be implemented by using hardware according to a general-purpose architecture (for example, an industrial personal computer based on a general-purpose personal computer). In this case, a plurality of operating systems (OSs) having different uses may be executed in parallel using a virtualization technology, and necessary applications may be executed on each OS.

(c2: Functional unit 200)

[0058] Fig. 4 is a schematic diagram illustrating a hardware configuration example of functional unit 200 constituting control system 2 according to the present embodiment. With reference to Fig. 4, functional unit 200 includes, as main components, a processor 202 such as a CPU or a GPU, a chipset 204, a volatile memory 206, a nonvolatile memory 208, a communication controller 210, and a communication interface 212, a memory card interface 214, network controllers 216 and 218, and an indicator 224.

[0059] Processor 202 reads various programs stored in nonvolatile memory 208, develops the programs in volatile memory 206, and executes the programs to imple-

ment various communication functions as described later. Chipset 204 mediates data exchange between processor 202 and each component, and thus implements the processing of functional unit 200 as a whole.

[0060] In addition to a system program, nonvolatile memory 208 stores various data such as a communication control program 232 that operates in an execution environment provided by the system program.

[0061] Communication controller 210 is in charge of exchanging data with control unit 100 and functional unit 300. As communication controller 210, for example, a communication chip corresponding to an internal bus, Ethernet, or the like can be adopted.

[0062] Communication interface 212 is in charge of exchanging data with an arbitrary information processing device via USB connection.

[0063] A memory card 215 is attachable to and detachable from memory card interface 214, and memory card interface 214 can write data such as a control program and various settings to memory card 215 or read data such as a control program and various settings from memory card 215.

[0064] Each of network controllers 216 and 218 is in charge of exchanging data with an arbitrary device via the network. Network controllers 216 and 218 may employ a general-purpose network protocol such as Ethernet. For example, functional unit 200 communicates with external device 500 via network controller 216 or network controller 218.

[0065] Indicator 224 notifies an operating state of functional unit 200 and the like and includes one or more LEDs disposed on a surface of the unit.

[0066] Although Fig. 4 illustrates the configuration example in which necessary functions are provided by processor 202 executing the programs, some or all of these provided functions may be implemented by using a dedicated hardware circuit (for example, ASIC or FPGA). Alternatively, a main part of functional unit 200 may be implemented by using hardware according to a general-purpose architecture (for example, an industrial personal computer based on a general-purpose personal computer). In this case, a plurality of OSs having different uses may be executed in parallel using a virtualization technology, and necessary applications may be executed on each OS.

(c3: Functional unit 300)

[0067] Fig. 5 is a schematic diagram illustrating a hardware configuration example of functional unit 300 constituting control system 2 according to the present embodiment. With reference to Fig. 5, functional unit 300 includes, as main components, a processor 302 such as a CPU or a GPU, a chipset 304, a volatile memory 306, nonvolatile memory 308, a memory card interface 314, an internal bus controller 322, and an indicator 324.

[0068] Processor 302 reads various application programs stored in nonvolatile memory 308, develops the application programs in volatile memory 306, executes the application programs to implement a server function and various functions. Chipset 304 mediates data exchange between processor 302 and each component, and thus implements the processing of functional unit 300 as a whole.

[0069] In addition to a system program, nonvolatile memory 308 stores an application program that operates in an execution environment provided by the system program and security information 330 (see Fig. 1).

[0070] A memory card 315 is attachable to and detachable from memory card interface 314, and memory card interface 314 can write data such as an application program and various settings to memory card 315 or read data such as an application program and various settings from memory card 315.

[0071] Internal bus controller 322 is in charge of exchanging data with control unit 100 and functional unit 200 via an internal bus.

[0072] Indicator 324 notifies an operating state of functional unit 300 and the like and includes one or more LEDs disposed on a surface of the unit.

[0073] Although Fig. 5 illustrates the configuration example in which necessary functions are provided by processor 302 executing the programs, some or all of these provided functions may be implemented by using a dedicated hardware circuit (for example, ASIC or FPGA). Alternatively, a main part of functional unit 300 may be implemented by using hardware according to a general-purpose architecture (for example, an industrial personal computer based on a general-purpose personal computer). In this case, a plurality of OSs having different uses may be executed in parallel using a virtualization technology, and necessary applications may be executed on each OS.

<D. Hardware configuration example of external device 500>

[0074] Next, a hardware configuration of external device 500 will be described in order with reference to Fig. 6. Fig. 6 is a schematic diagram illustrating a hardware configuration example of external device 500 constituting information processing system 1 according to the embodiment.

[0075] For example, external device 500 includes a computer configured in accordance with a general-purpose computer architecture. External device 500 includes a processor 502 such as a CPU or MPU, a volatile memory 504, a nonvolatile memory 510, a communication interface 511, an input/output (I/O) interface 514, and a display interface 520. These components are communicably connected to each other via an internal bus 525.

[0076] Processor 502 controls an operation of external device 500 by executing various control programs such as a development support program 510A and a browser application (not shown). Development support program 510A is a program that provides an environment for de-

veloping a control program (user program) of control system 2. Processor 502 reads the control program to be executed from nonvolatile memory 510 to volatile memory 504 in response to reception of execution instructions of various control programs such as development support program 510A and the browser application.

[0077] Communication interface 511 exchanges data with other communication devices via a network. The other communication devices include, for example, functional unit 200, a server, and the like. External device 500 may be configured to download various control programs such as development support program 510A from the other communication devices via communication interface 511.

[0078] I/O interface 514 is connected to input device 515 and captures a signal indicating a user operation from input device 515. Input device 515 typically includes a keyboard, a mouse, a touch panel, a touch pad, and the like, and accepts operations from the user. In the example in Fig. 6, external device 500 and input device 515 are shown as separate bodies, but external device 500 and input device 515 may be integrally configured.

[0079] Display interface 520 is connected to a display 521 and sends an image signal for displaying an image to display 521 in response to a command from processor 502 or the like. Display 521 is, for example, a liquid crystal display (LCD) or an organic electro luminescence (EL) display and presents various information to the user. Display 521 may display various screens provided by development support program 510A. In the example in Fig. 6, external device 500 and display 521 are shown as separate bodies, but external device 500 and display 521 may be integrally configured.

<E. Unit configuration example of information processing system 1>

[0080] Fig. 7 is a diagram illustrating an example of a unit configuration of information processing system 1. A specific example of the unit configuration of information processing system 1 will be described with reference to Fig. 7.

[0081] As shown in Fig. 7, information processing system 1 includes control system 2 and external device 500. Control system 2 includes control unit 100, functional units 200A and 200B, and functional unit 300. Functional units 200A and 200B are examples of functional unit 200 (see Fig. 2). Control unit 100, functional units 200A and 200B, and functional unit 300 are connected to each other via internal bus 10. These units communicate with each other via internal bus 10. The communication is achieved by, for example, virtual Ethernet.

[0082] Functional unit 200 and external device 500 are connected to an external network NW1. An IP address "192.168.250.3" is assigned to external device 500. Functional unit 200 and external device 500 each have a physical communication port and are connected to external network NW1 via the communication port.

[0083] Control unit 100 and functional units 200A, 200B, and 300 are connected to an internal network NW2. A virtual IP address "192.168.250.1" is assigned to control unit 100. Further, a unit name "Unit #0" is assigned to control unit 100.

[0084] An IP address "192.168.250.2" is assigned to functional unit 200A. A unit name "Unit #1" is assigned to functional unit 200A. Functional unit 200A functions as a web server "Web1". Applications "App11" and "App12" are installed in functional unit 200A. Applications "App11" and "App12" are accessed from web server "Web1".

[0085] A virtual IP address "192.168.251.100" is assigned to functional unit 200B. In addition, a unit name "Unit #2" is assigned to functional unit 200B. Functional unit 200B functions as a web server "Web2". Applications "App21" and "App22" are installed in functional unit 200B. Applications "App21" and "App22" are accessed from web server "Web2".

[0086] A virtual IP address "192.168.251.101" is assigned to functional unit 300. In addition, a unit name "Unit #3" is assigned to functional unit 300. Functional unit 300 functions as a web server "Web3". Applications "App31" and "App32" are installed in functional unit 300. Applications "App31" and "App32" are accessed from web server "Web3".

<F. Sequence flow>

[0087] Next, a control flow of control system 2 will be described with reference to Figs. 8 to 10. Fig. 8 is a diagram illustrating a data flow between functional unit 200, functional unit 300, and external device 500.

[0088] In step S20, it is assumed that control system 2 is started. On the basis of this start, a master-slave relationship is established between functional units 200 and 300. The master-slave relationship may be set in advance or may be arbitrarily set by the user. In the example in Fig. 8, it is assumed that functional unit 200 is set as a slave unit and functional unit 300 is set as a master unit. Functional unit 200 as a slave unit sends a request for acquisition of security information 330 to functional unit 300 as a master unit. Functional unit 300 sends security information 330 to functional unit 200 on the basis of receipt of the request for acquisition.

[0089] In step S22, functional unit 200 stores security information 330 received from functional unit 300 in volatile memory 206.

[0090] In step S30, it is assumed that external device 500 receives a request for data access to functional unit 200 from the user. At time of step S30, a login process to functional unit 200 has not been performed, and external device 500 is requested to input the account information. Specifically, functional unit 200 sends a URL of a login page to external device 500 on the basis of the request for data access received from external device 500, and redirects the user to the login page.

[0091] In step S32, external device 500 sends the re-

quest for access to the login page to functional unit 200 on the basis of the URL received from functional unit 200. On the basis of this request, functional unit 200 sends the accessed login page to external device 500.

[0092] In step S34, external device 500 displays the login page received from functional unit 200 on display 521 (see Fig. 6). Fig. 9 is a diagram illustrating an example of a screen displayed on external device 500. In Fig. 9, a login page 700 is shown as an example of the screen displayed on external device 500. Login page 700 accepts input of account information such as a user ID and a password. When a login button on login page 700 is pressed, the entered account information is sent to functional unit 200. When a cancel button on login page 700 is pressed, the entered account information is discarded, and login page 700 is closed.

[0093] In step S36, it is assumed that the login button on login page 700 is pressed. As a result, external device 500 sends the account information entered on login page 700 to functional unit 200.

[0094] In step S50, functional unit 200 authenticates the account information by referring to security information 330 (see Fig. 1) stored in volatile memory 206 on the basis of receipt of the account information from external device 500. In a case where the account information input to external device 500 is registered in security information 330 stored in volatile memory 206, functional unit 200 allows external device 500 to access data in functional unit 200.

[0095] Fig. 10 is a diagram of registered account information 330A included in security information 330. Registered account information 330A associates a password and the like with each user ID. Functional unit 200 acquires the password corresponding to the user ID from registered account information 330A by using the user ID included in input account information received from external device 500 as a key. Next, functional unit 200 compares the password acquired from registered account information 330A with the password included in the input account information received from external device 500. When these passwords match, functional unit 200 determines that the input account information received from external device 500 is registered in registered account information 330A.

[0096] In step S52, functional unit 200 sends a HyperText Markup Language (HTML) document of a portal site to external device 500 as a response to the request for data access in step S30.

[0097] In step S54, external device 500 configures a portal site on the basis of the received HTML document and displays the portal site on display 521 (see Fig. 6). Fig. 9 illustrates an example of a portal site 710 displayed on external device 500.

[0098] Portal site 710 provides a hyperlink with a link to the application installed on functional unit 200. In the example in Fig. 9, the link to application "App11" (see Fig. 7) installed on functional unit 200 is shown as a hyperlink 710A, and application "App12" (see Fig. 7) installed on functional unit 200) is shown as a hyperlink 710B. The user can use a function of application "App11" by selecting hyperlink 710A and can use a function of application "App12" by selecting hyperlink 710B.

<G. First modification>

[0099] Next, modifications of control system 2 will be described with reference to Figs. 11 and 12. Fig. 11 is a diagram illustrating a configuration example of a control system 2A according to a first modification.

[0100] In control system 2, functional unit 200 as a slave unit uses security information 330 distributed from functional unit 300 as a master unit. On the other hand, in control system 2A according to this modification, functional unit 200 not only uses security information 330 received from functional unit 300, but also uses security information 230 stored in advance in functional unit 200. Since the other points are as described above, the duplicated description will not be repeated below.

[0101] As shown in Fig. 11, security information 230 is stored in advance in nonvolatile memory 208 of functional unit 200. Further, functional unit 200 stores security information 330 distributed from functional unit 300 in volatile memory 206. As a result, functional unit 200 has security information 230 and security information 330.

[0102] Functional unit 200 merges security information 230 and security information 330. Fig. 12 is a diagram illustrating a process of merging security information 230 and security information 330. Specifically, Fig. 12 illustrates registered account information 230A included in security information 230, registered account information 330A included in security information 330, and a merge result 233 of registered account information 230A and 330A.

[0103] As shown in Fig. 12, information may conflict between information included in security information 230 and information included in security information 330. The term "conflict" as used herein means that unique information such as a user ID is duplicated. In the example in Fig. 12, a user ID "user2" included in registered account information 230A and a user ID "user2" included in registered account information 330A conflict with each other.

[0104] Functional unit 200 determines which of the conflicting information to prioritize in accordance with a merge rule when the information conflicts between the information included in security information 230 (first security information) and the information included in security information 330 (second security information).

[0105] For example, a priority is set in advance for each functional unit, and functional unit 200 prioritizes information acquired from the unit having a high priority. For example, it is assumed that the priority is set such that the priority of functional unit 300 as a master unit is higher than as a slave unit. In this case, functional unit 200 prioritizes security information 330 received from functional unit 300 over security information 230 stored in functional unit 200. As a result, the account information of user ID

"user2" and a password "pass2A" is prioritized over the account information of user ID "user2" and a password "pass2B". This prevents conflicts of the account information.

<H. Second modification>

[0106] Next, another modification of control system 2 will be described with reference to Fig. 13. Fig. 13 is a diagram illustrating a configuration example of a control system 2B according to a second modification.

[0107] In control system 2, the master unit distributes the security information to the slave units. On the other hand, in control system 2B according to this modification, not only the master unit distributes security information to the slave units, but also the slave units distribute security information to the other units. Since the other points are as described above, the duplicated description will not be repeated below.

[0108] As shown in Fig. 13, control unit 100 as a slave unit, has a volatile memory 106 and a nonvolatile memory 108. Security information 130 is stored in nonvolatile memory 108 in advance.

[0109] Functional unit 200 as a slave unit has a volatile memory 206 and a nonvolatile memory 208. Security information 230 is stored in advance in volatile memory 206.

[0110] Functional unit 300 as a master unit has a volatile memory 306 and a nonvolatile memory 308. Security information 330 is stored in advance in volatile memory 306.

[0111] Control unit 100 distributes security information 130 stored in nonvolatile memory 108 to functional units 200 and 300 at a predetermined timing. Functional unit 200 stores security information 130 received from control unit 100 in volatile memory 206. Similarly, functional unit 300 stores security information 130 received from control unit 100 in volatile memory 306.

[0112] Functional unit 200 distributes security information 230 stored in nonvolatile memory 208 to control unit 100 and functional unit 300 at a predetermined timing. Control unit 100 stores security information 230 received from functional unit 200 in volatile memory 106. Similarly, functional unit 300 stores security information 230 received from functional unit 200 in volatile memory 306.

[0113] Functional unit 300 distributes security information 330 stored in nonvolatile memory 208 to control unit 100 and functional unit 200 at a predetermined timing. Control unit 100 stores security information 330 received from functional unit 300 in volatile memory 106. Similarly, functional unit 200 stores security information 330 received from functional unit 300 in volatile memory 206.

[0114] The timing at which security information 130, 230, and 330 is distributed to other units is not limited. In a certain aspect, security information 130, 230, and 330 is distributed to each unit at a timing at which power of control system 2B is turned on. In another aspect, security information 130, 230, and 330 is distributed to each unit at predetermined intervals. In still another aspect, security information 130, 230, and 330 is distributed to each unit at a timing of receiving an acquisition instruction or update instruction by a user operation.

[0115] After receiving the security information from the other units, each unit of control unit 100 and functional units 200 and 300 merges security information 130, 230, and 330 in accordance with a predetermined merge rule. At this time, when information conflicts between security information 130, 230, and 330, each unit resolves the information conflict by a method described in "G. First modification".

[0116] Although in Fig. 13, the example has been described in which the security information is distributed to all the other units, the security information does not have to be distributed to all the other units. For example, a unit that allows distribution of the security information and a unit that prohibits distribution of the security information are predetermined, and each unit may distribute the security information only to other units that are allowed to distribute the security information.

<I. Third modification>

[0117] Next, another modification of control system 2 will be described with reference to Figs. 14 and 15. Fig. 14 is a diagram illustrating a configuration example of a control system 2C according to a third modification.

[0118] In the above, the example in which security information 330 includes the account information has been described. On the other hand, in this modification, security information 330 includes key information 330B such as a private key and a digital certificate used for encryption. Since the other points are as described above, the duplicated description will not be repeated below.

[0119] As shown in Fig. 14, security information 330 including key information 330B is stored in nonvolatile memory 308 of functional unit 300 as a master unit. Fig. 15 is a diagram of key information 330B included in security information 330. Key information 330B includes one or more sets of a digital certificate and a private key.

[0120] The digital certificate includes a public key used for encryption. A digital certificate is a data set for certifying an owner of the public key. Typically, digital certificates are pre-issued by a certification body called a certificate authority (CA).

[0121] With reference to Fig. 14 again, functional unit 300 as a master unit sends security information 330 including key information 330B to control unit 100 and functional unit 200 as slave units at a predetermined timing. Control unit 100 stores security information 330 received from functional unit 300 in volatile memory 106. Similarly, functional unit 200 stores security information 330 received from functional unit 300 in volatile memory 206.

[0122] Each unit constituting control system 2C achieves secure communication with external device 500 by using key information 330B held by each unit. Fig. 14 illustrates an example in which functional unit 200 is per-

forming secure communication with an external device 500A and an example in which functional unit 300 is performing secure communication with an external device 500B.

[0123] For example, functional units 200 and 300 achieve secure communication with external devices 500A and 500B by Secure Sockets Layer (SSL) communication.

[0124] Specifically, functional unit 200 as a slave unit sends a digital certificate C1 stored in volatile memory 206 to external device 500A in response to reception of a request for acquisition of data stored in functional unit 200 from external device 500A. Digital certificate C1 generally includes a host name of a registrant. As described above, digital certificate C1 is distributed from functional unit 300, but when the host name specified in digital certificate C1 is functional unit 300 although a sender of digital certificate C1 is functional unit 200, external device 500A cannot authenticate the sender correctly. Thus, a multi-domain certificate or a wildcard certificate is used as digital certificate C1. A multi-domain certificate is a certificate that can authenticate multiple domains with one digital certificate C1. A wildcard certificate is a certificate that can authenticate all subdomains belonging to the same hierarchy of "*." by adding "*." as a common name.

[0125] External device 500A verifies digital certificate C1 received from functional unit 200 and determines whether the sender of digital certificate C1 is a legitimate sender. When external device 500A determines that the sender of digital certificate C1 is a legitimate sender, external device 500A generates a common key (not shown). After that, external device 500A encrypts the generated common key using the public key included in digital certificate C1 and sends the encrypted common key to functional unit 200.

[0126] In response to reception of the encrypted common key from external device 500A, functional unit 200 decrypts the common key by using a private key K1 included in key information 330B. By the above processing, the common key is safely sent from functional unit 200 to external device 500A. In the subsequent communication, functional unit 200 and external device 500A encrypt data using the common key and then exchange the data with each other.

[0127] Similarly, functional unit 300 uses key information 330B stored in nonvolatile memory 308 to perform SSL communication with external device 500B.

<J. Appendix>

[0128] As described above, the present embodiment includes the following disclosure.

[Configuration 1]

[0129] A control system (2) comprising a plurality of units, wherein

the plurality of units comprise
a master unit (300) connected to a bus (10), and
a slave unit (200) connected to the bus (10) and configured to communicate with the master unit (300) via the bus (10),
the master unit (300) comprises a nonvolatile memory (308) configured to store first security information (330) as information to be concealed,
the slave unit (200) comprises a volatile memory (206), and
the slave unit (200) is configured to receive the first security information (330) from the master unit (300) at a predetermined timing and store the first security information (330) in the volatile memory (206).

[Configuration 2]

[0130] The control system according to configuration 1, wherein the predetermined timing includes a timing at which power of control system (2) is turned on.

[Configuration 3]

[0131] The control system according to configuration 1 or 2, wherein

the first security information (330) includes account information of a user,
in response to reception of a request for data access to slave unit (200) from an external device (500) configured to be communicable with the slave unit (200), the slave unit (200) requests the external device (500) to input account information, and
in a case where the account information input to the external device (500) is registered in the first security information (330) stored in the volatile memory (206), the slave unit (200) allows data access to the slave unit (200) by the external device (500).

[Configuration 4]

[0132] The control system according to any one of configurations 1 to 3, wherein

the first security information (330) includes a digital certificate, and
in response to reception of a request for acquisition of data stored in slave unit (200) from the external device (500) configured to be communicable with the slave unit (200), the slave unit (200) sends the digital certificate stored in the volatile memory (206) to the external device (500).

[Configuration 5]

[0133] The control system according to any one of configurations 1 to 4, wherein

the slave unit (200) further comprises a nonvolatile memory (208) configured to store second security information (230) as information to be concealed, and
in a case where there is conflicting information between information included in the first security information (330) and information included in the second security information (230), the slave unit (200) determines which of the conflicting information to prioritize in accordance with a predetermined rule.

[Configuration 6]

[0134] The control system according to configuration 5, wherein the master unit (300) is configured to receive the second security information (230) from the slave unit (200) at the predetermined timing and store the second security information (230) in the volatile memory (306) of the master unit (300).

[Configuration 7]

[0135] The control system according to any one of configurations 1 to 6, wherein
the slave unit (200) comprises a control unit (100) that controls a drive device.

[Configuration 8]

[0136] A control method of a control system (2) includes a plurality of units,

the plurality of units comprising

a master unit (300) connected to a bus (10), and a slave unit (200) connected to the bus (10) and configured to communicate with master unit (300) via bus (10),

the control method comprising:

storing, by master unit (300), first security information (330) as information to be concealed in a nonvolatile memory (308) of the master unit (300),
receiving, by slave unit (200), the first security information (330) from the master unit (300) at a predetermined timing, and
storing, by slave unit (200), the first security information (330) received from the master unit (300) in a volatile memory (206) of the slave unit (200).

[0137] It should be understood that the embodiment disclosed herein is illustrative in all respects and not restrictive. The scope of the present invention is defined not by the above description but by the claims and is intended to include meanings equivalent to the claims and all modifications within the scope.

REFERENCE SIGNS LIST

[0138] 1: Information processing system, 2, 2A, 2B, 2C: Control system, 10, 525: Internal bus, 100: Control unit, 102, 202, 302, 502: Processor, 104, 204, 304: Chipset, 106, 206, 306, 504: Volatile memory, 108, 208, 308, 510: Nonvolatile memory, 110, 210: Communication controller, 112: USB controller, 114, 214, 314: Memory card interface, 115, 215, 315: Memory card, 116, 118, 120, 216, 218: Network controller, 122, 322: Internal bus controller, 124, 224, 324: Indicator, 130, 230, 330: Security information, 200, 200A, 200B, 300, 400: Functional unit, 212, 511: Communication interface, 230A, 330A: Registered account information, 232: Communication control program, 233: Merge result, 330B: Key information, 450: Power supply unit, 500, 500A, 500B: External device, 510A: Development support program, 514: Interface, 515: Input device, 520: Display interface, 521: Display, 700: Login page, 710: Portal site, 710A, 710B: Hyperlink.

Claims

1. A control system comprising a plurality of units, wherein

   the plurality of units comprise

   a master unit connected to a bus, and
   a slave unit connected to the bus and configured to communicate with the master unit via the bus,

   the master unit comprises a nonvolatile memory configured to store first security information as information to be concealed,

   the slave unit comprises a volatile memory, and
   the slave unit is configured to receive the first security information from the master unit at a predetermined timing and store the first security information in the volatile memory.

2. The control system according to claim 1, wherein the predetermined timing includes a timing at which power of the control system is turned on.

3. The control system according to claim 1 or 2, wherein

   the first security information includes account information of a user,
   in response to reception of a request for data access to the slave unit from an external device

configured to be communicable with the slave unit, the slave unit requests the external device to input account information, and
in a case where the account information input to the external device is registered in the first security information stored in the volatile memory, the slave unit allows data access to the slave unit by the external device.

4. The control system according to any one of claims 1 to 3, wherein

the first security information includes a digital certificate, and
in response to reception of a request for acquisition of data stored in the slave unit from the external device configured to be communicable with the slave unit, the slave unit sends the digital certificate stored in the volatile memory to the external device.

5. The control system according to any one of claims 1 to 4, wherein

the slave unit further comprises a nonvolatile memory configured to store second security information as information to be concealed, and
in a case where there is conflicting information between information included in the first security information and information included in the second security information, the slave unit determines which of the conflicting information to prioritize in accordance with a predetermined rule.

6. The control system according to claim 5, wherein the master unit is configured to receive the second security information from the slave unit at the predetermined timing and store the second security information in the volatile memory of the master unit.

7. The control system according to any one of claims 1 to 6, wherein the slave unit comprises a control unit that controls a drive device.

8. A control method of a control system including a plurality of units,

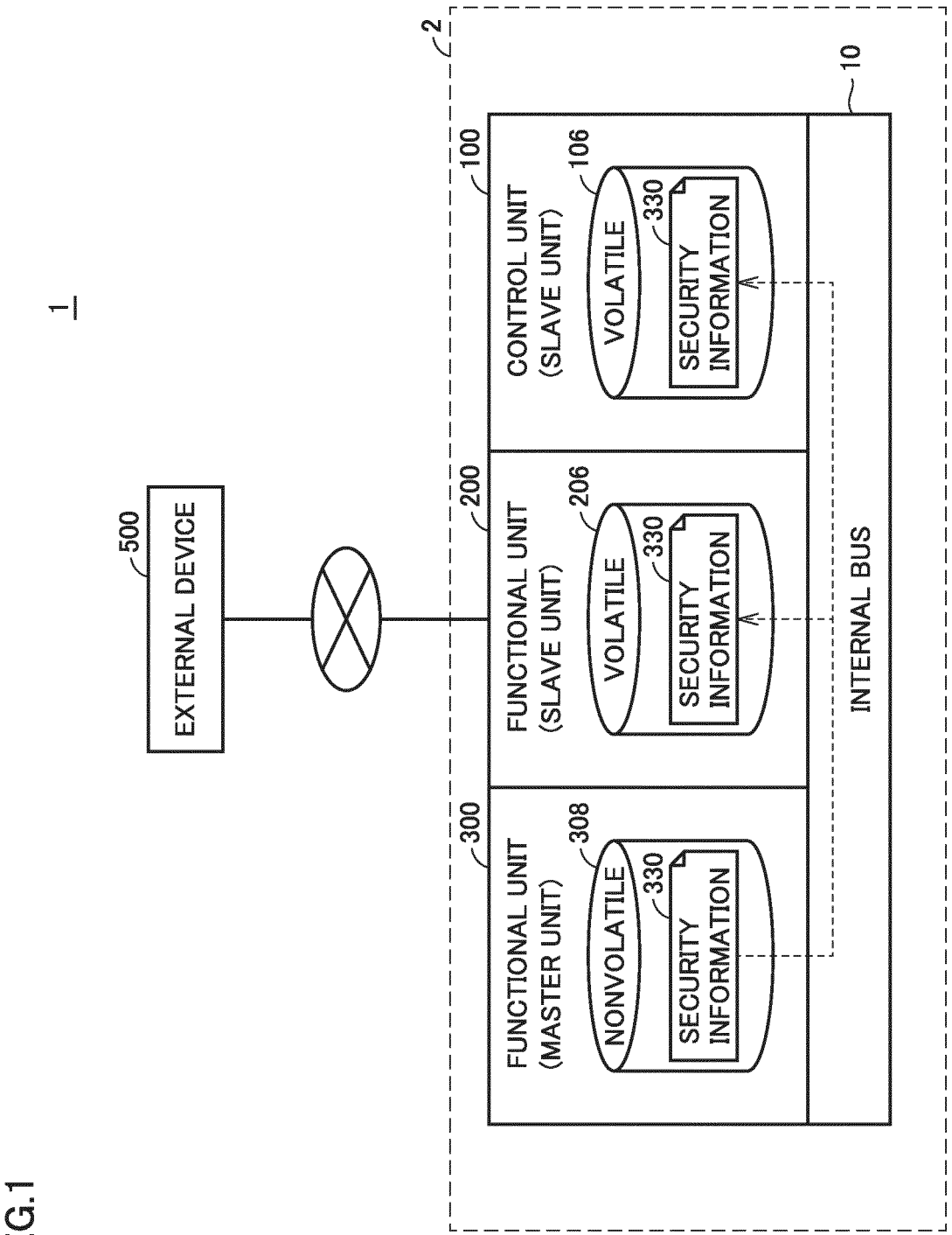
the plurality of units comprising

a master unit connected to a bus, and
a slave unit connected to the bus and configured to communicate with the master unit via the bus,

the control method comprising:

storing, by the master unit, first security information as information to be concealed in a nonvolatile memory of the master unit;
receiving, by the slave unit, the first security information from the master unit at a predetermined timing; and
storing, by the slave unit, the first security information received from the master unit in a volatile memory of the slave unit.

FIG.1


1
2
10
INTERNAL BUS
500
EXTERNAL DEVICE
100
CONTROL UNIT
(SLAVE UNIT)
106
VOLATILE
330
SECURITY
INFORMATION
200
FUNCTIONAL UNIT
(SLAVE UNIT)
206
VOLATILE
330
SECURITY
INFORMATION
300
FUNCTIONAL UNIT
(MASTER UNIT)
308
NONVOLATILE
330
SECURITY
INFORMATION

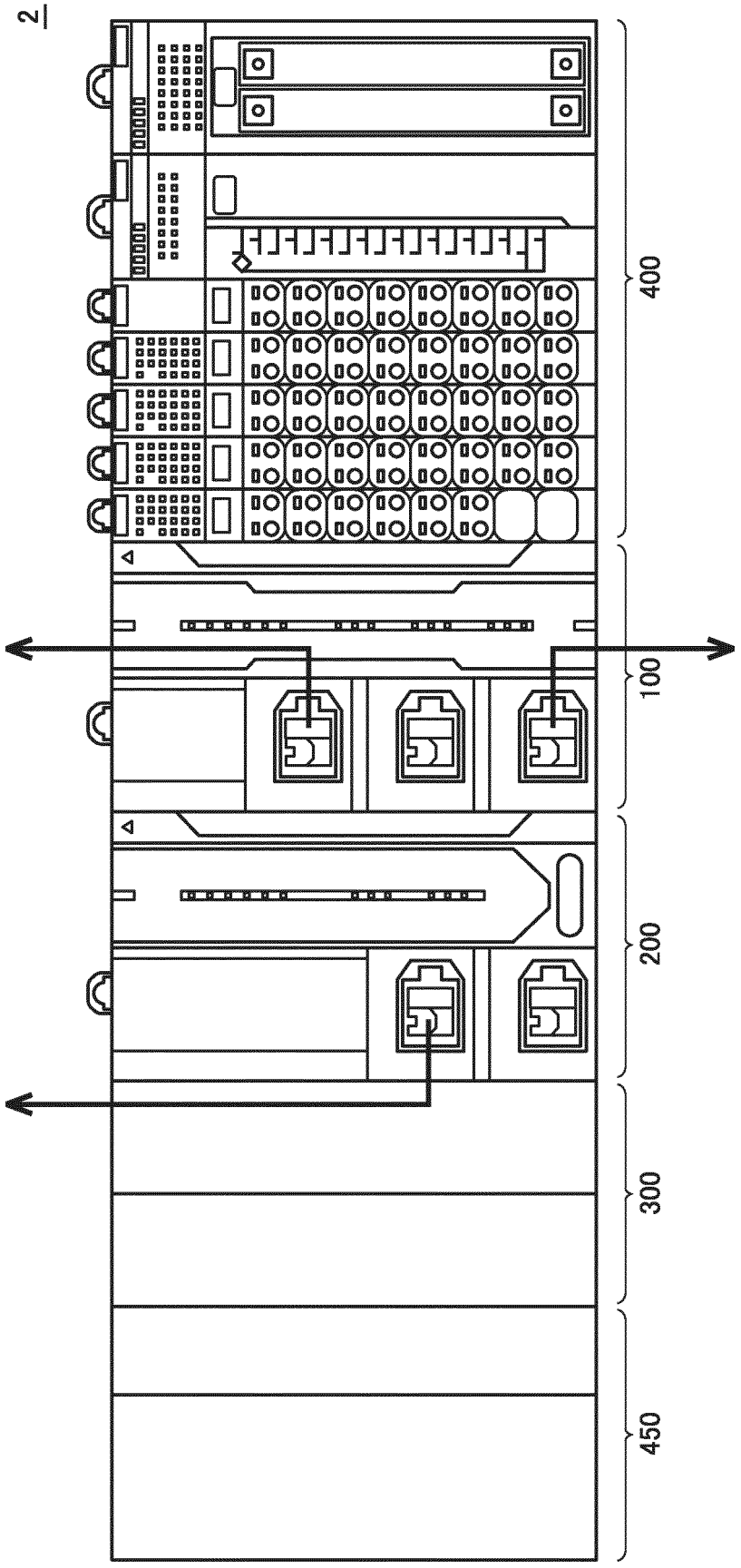


FIG.2

FIG.3

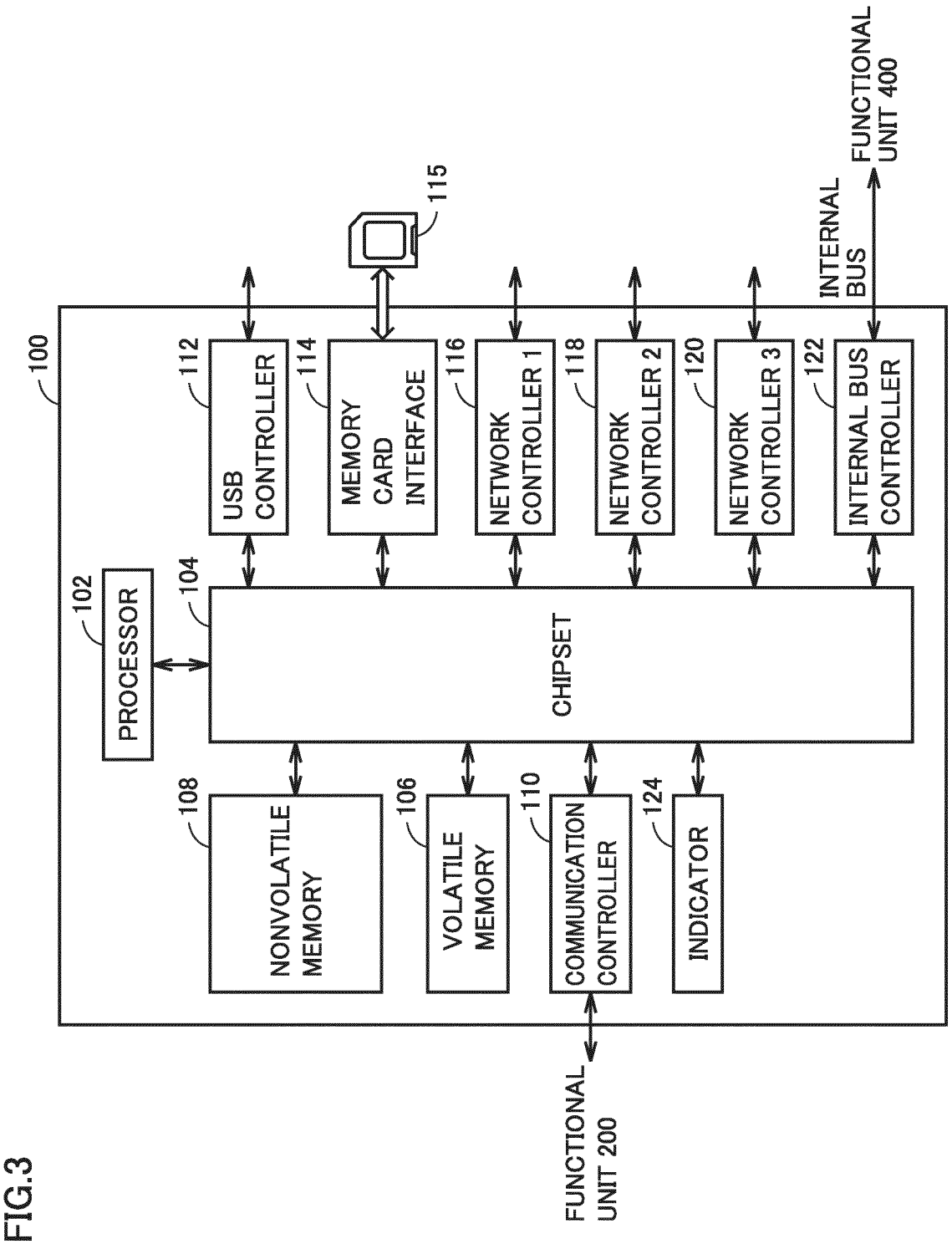

100
102
PROCESSOR
104
CHIPSET
108
NONVOLATILE MEMORY
106
VOLATILE MEMORY
110
COMMUNICATION CONTROLLER
124
INDICATOR
112
USB CONTROLLER
114
MEMORY CARD INTERFACE
115
116
NETWORK CONTROLLER 1
118
NETWORK CONTROLLER 2
120
NETWORK CONTROLLER 3
122
INTERNAL BUS CONTROLLER
INTERNAL BUS
FUNCTIONAL UNIT 400
FUNCTIONAL UNIT 200

FIG.4

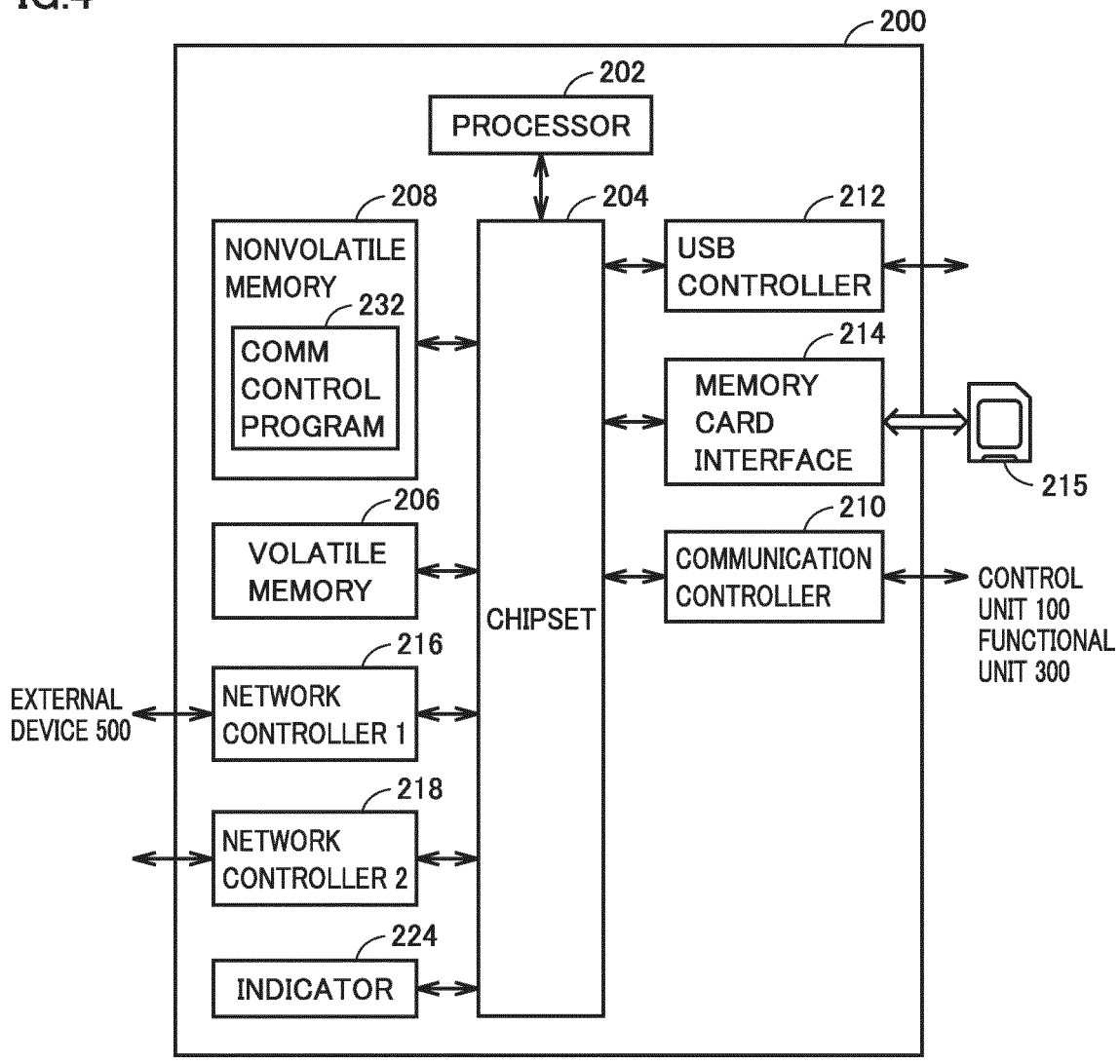

200
202
PROCESSOR
208
NONVOLATILE MEMORY
232
COMM CONTROL PROGRAM
204
CHIPSET
212
USB CONTROLLER
214
MEMORY CARD INTERFACE
215
206
VOLATILE MEMORY
210
COMMUNICATION CONTROLLER
CONTROL UNIT 100 FUNCTIONAL UNIT 300
216
EXTERNAL DEVICE 500
NETWORK CONTROLLER 1
218
NETWORK CONTROLLER 2
224
INDICATOR

FIG.5

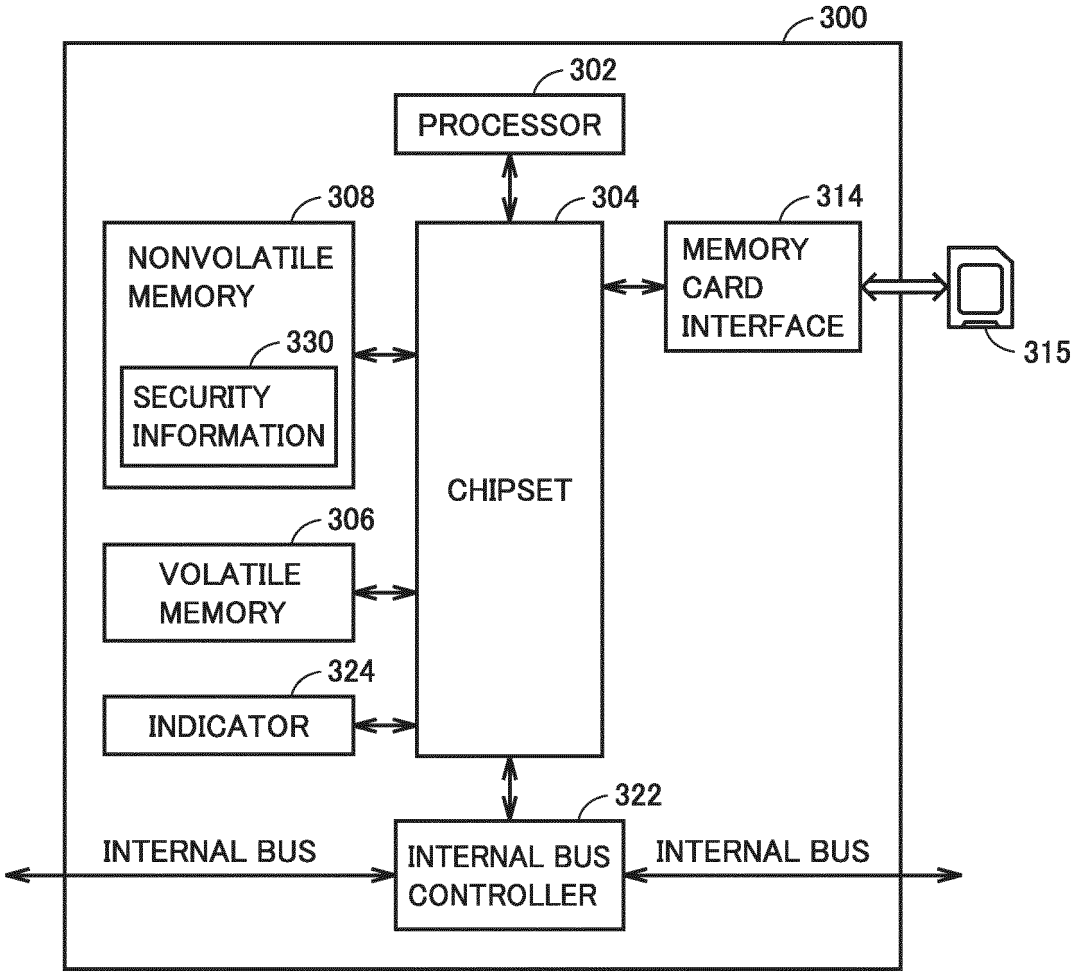

300
302
PROCESSOR
308
NONVOLATILE MEMORY
330
SECURITY INFORMATION
304
CHIPSET
314
MEMORY CARD INTERFACE
315
306
VOLATILE MEMORY
324
INDICATOR
322
INTERNAL BUS
INTERNAL BUS CONTROLLER
INTERNAL BUS

FIG.6

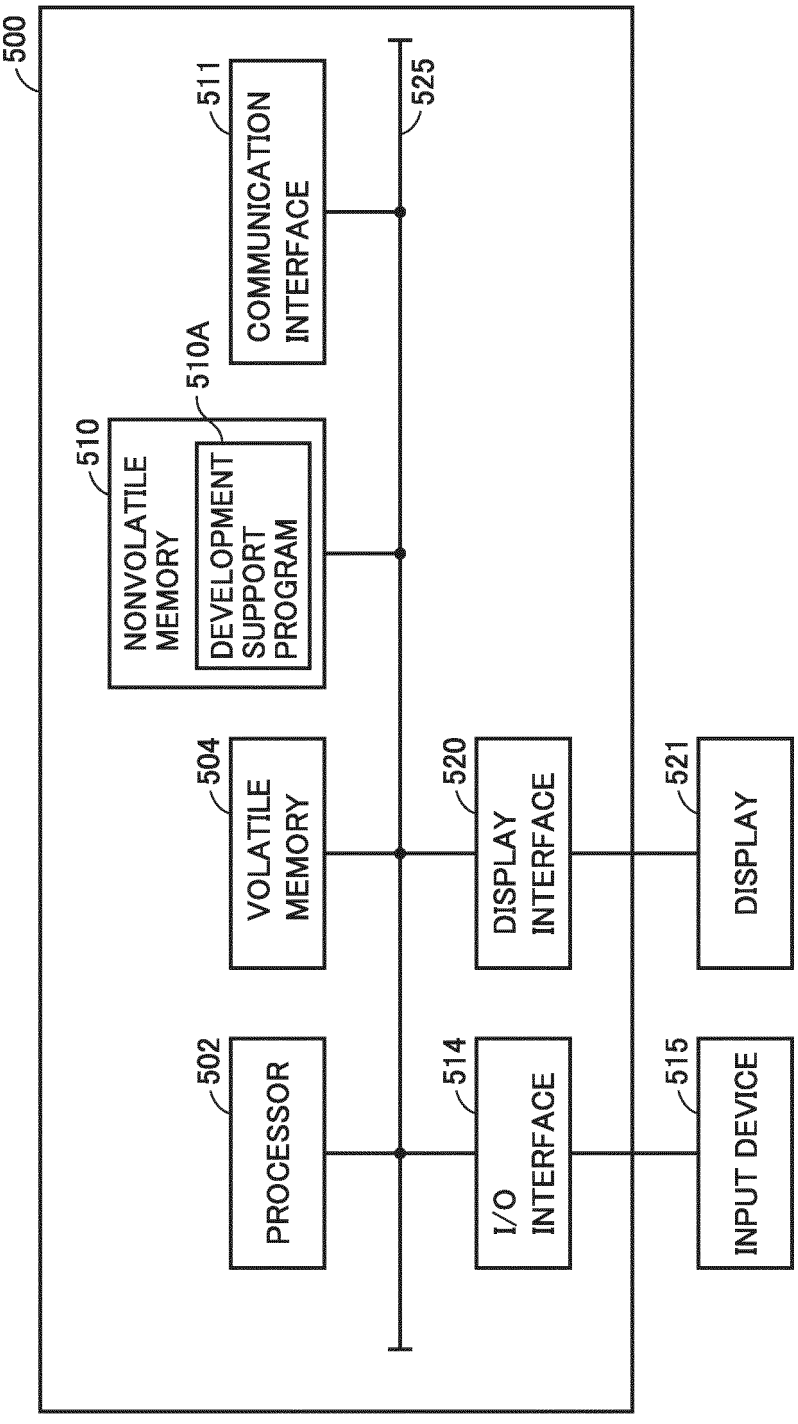

500
511
COMMUNICATION INTERFACE
525
510A
510
NONVOLATILE MEMORY
DEVELOPMENT SUPPORT PROGRAM
504
VOLATILE MEMORY
520
DISPLAY INTERFACE
521
DISPLAY
502
PROCESSOR
514
I/O INTERFACE
515
INPUT DEVICE

FIG.7

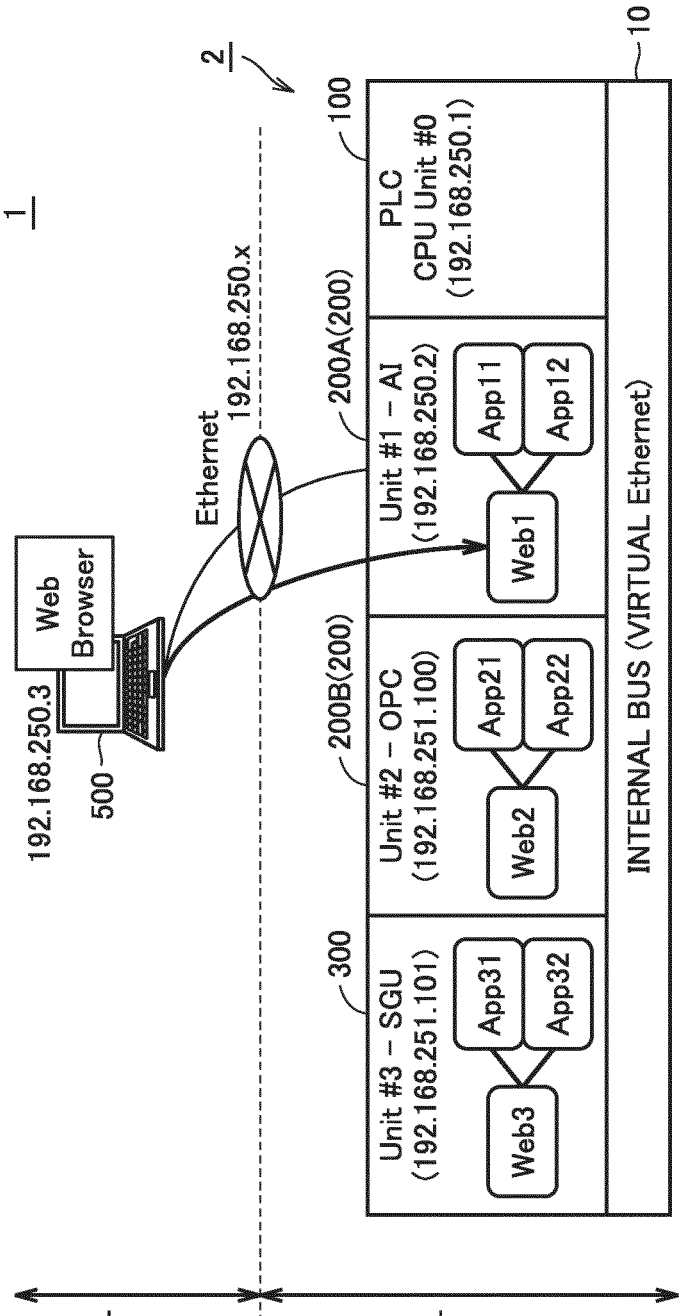

1
2
10
100
PLC
CPU Unit #0
(192.168.250.1)
200A(200)
Unit #1 – AI
(192.168.250.2)
App11
App12
Web1
200B(200)
Unit #2 – OPC
(192.168.251.100)
App21
App22
Web2
300
Unit #3 – SGU
(192.168.251.101)
App31
App32
Web3
INTERNAL BUS (VIRTUAL Ethernet)
Ethernet
192.168.250.x
Web
Browser
192.168.250.3
500
EXTERNAL
NETWORK
NW1
EXTERNAL
NETWORK
NW2

FIG.8

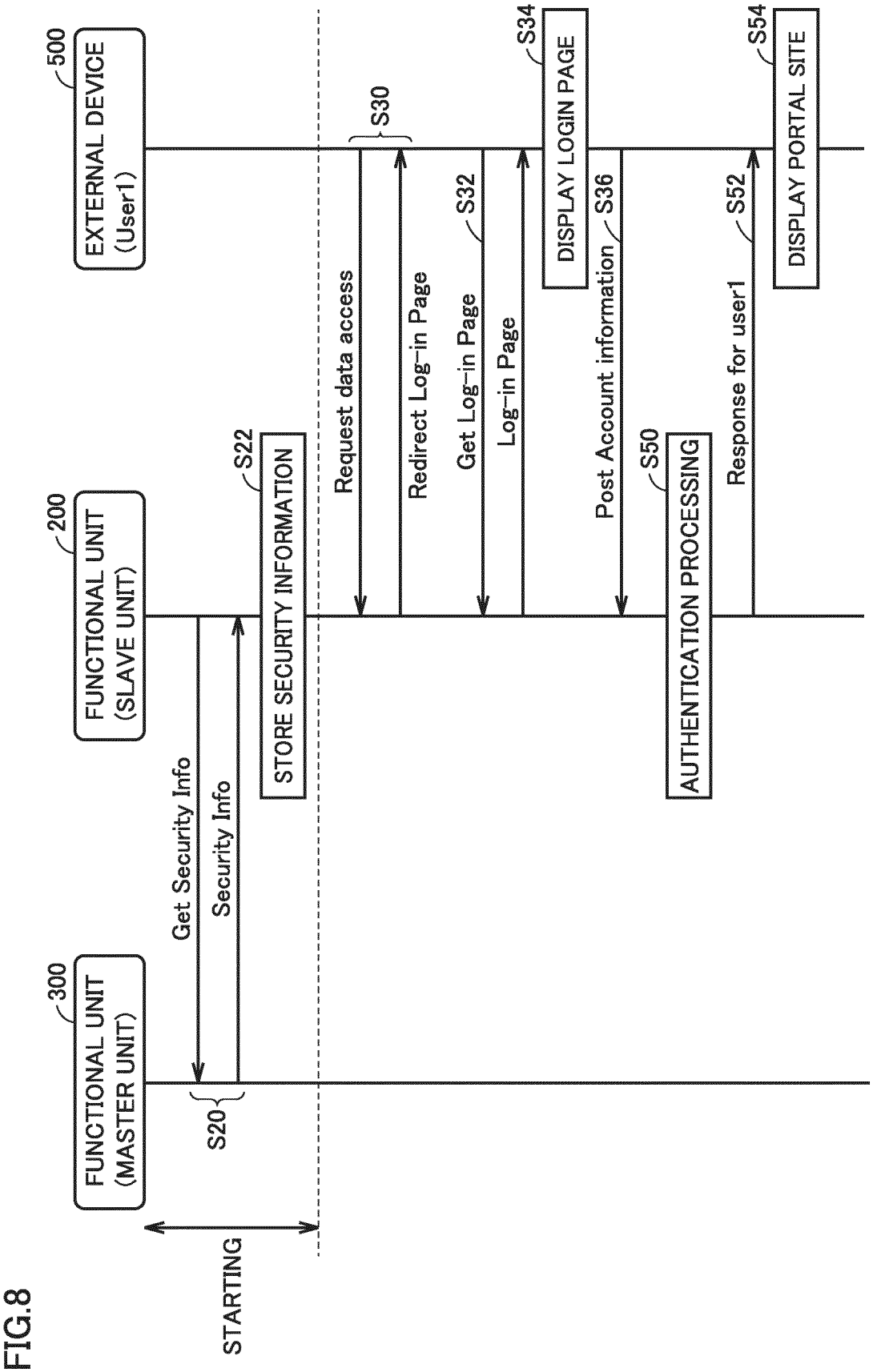

500
EXTERNAL DEVICE (User1)
200
FUNCTIONAL UNIT (SLAVE UNIT)
300
FUNCTIONAL UNIT (MASTER UNIT)
STARTING
S20
Get Security Info
Security Info
S22
STORE SECURITY INFORMATION
S30
Request data access
Redirect Log-in Page
S32
Get Log-in Page
Log-in Page
S34
DISPLAY LOGIN PAGE
S36
Post Account information
S50
AUTHENTICATION PROCESSING
S52
Response for user1
S54
DISPLAY PORTAL SITE

FIG.9

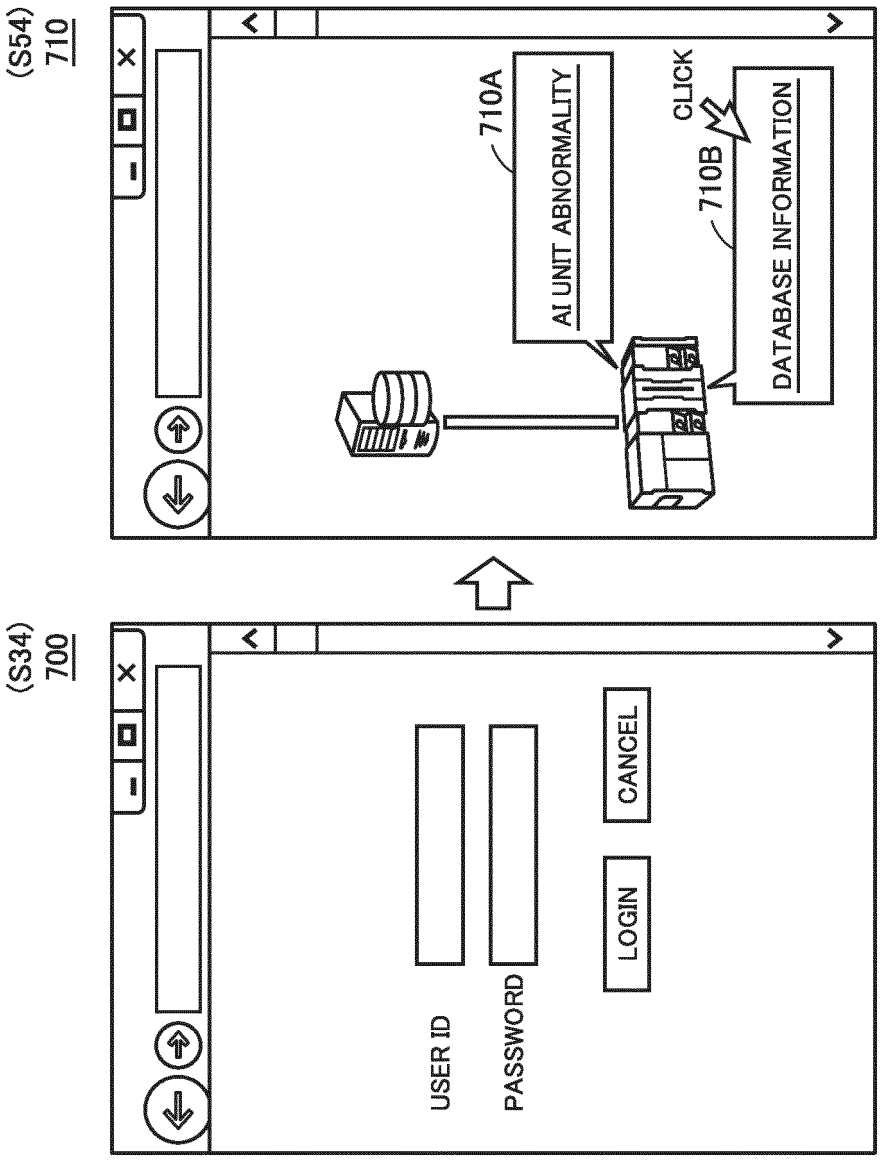

(S34)
700
USER ID
PASSWORD
LOGIN
CANCEL
(S54)
710
710A
AI UNIT ABNORMALITY
CLICK
710B
DATABASE INFORMATION

FIG.10

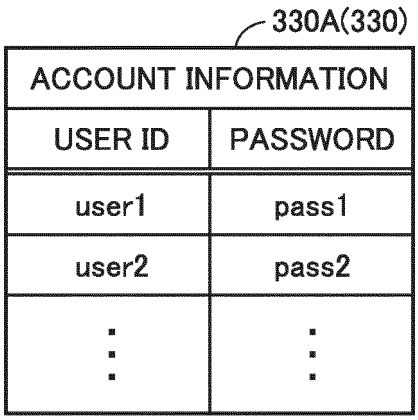

330A(330)
ACCOUNT INFORMATION
USER ID
PASSWORD
user1
pass1
user2
pass2

FIG.11

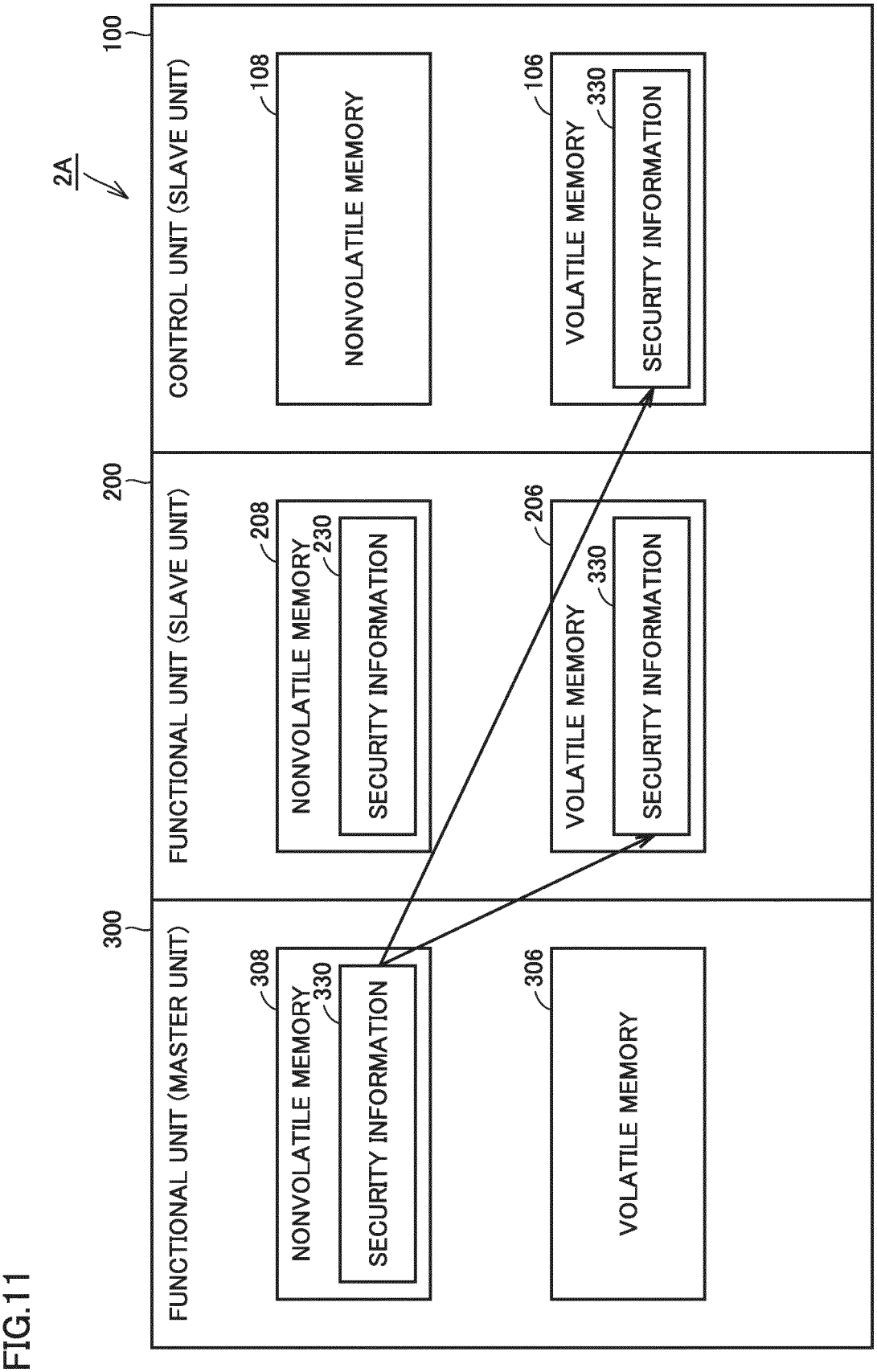

2A
100
CONTROL UNIT (SLAVE UNIT)
108
NONVOLATILE MEMORY
106
VOLATILE MEMORY
330
SECURITY INFORMATION
200
FUNCTIONAL UNIT (SLAVE UNIT)
208
NONVOLATILE MEMORY
230
SECURITY INFORMATION
206
VOLATILE MEMORY
330
SECURITY INFORMATION
300
FUNCTIONAL UNIT (MASTER UNIT)
308
NONVOLATILE MEMORY
330
SECURITY INFORMATION
306
VOLATILE MEMORY

FIG.12

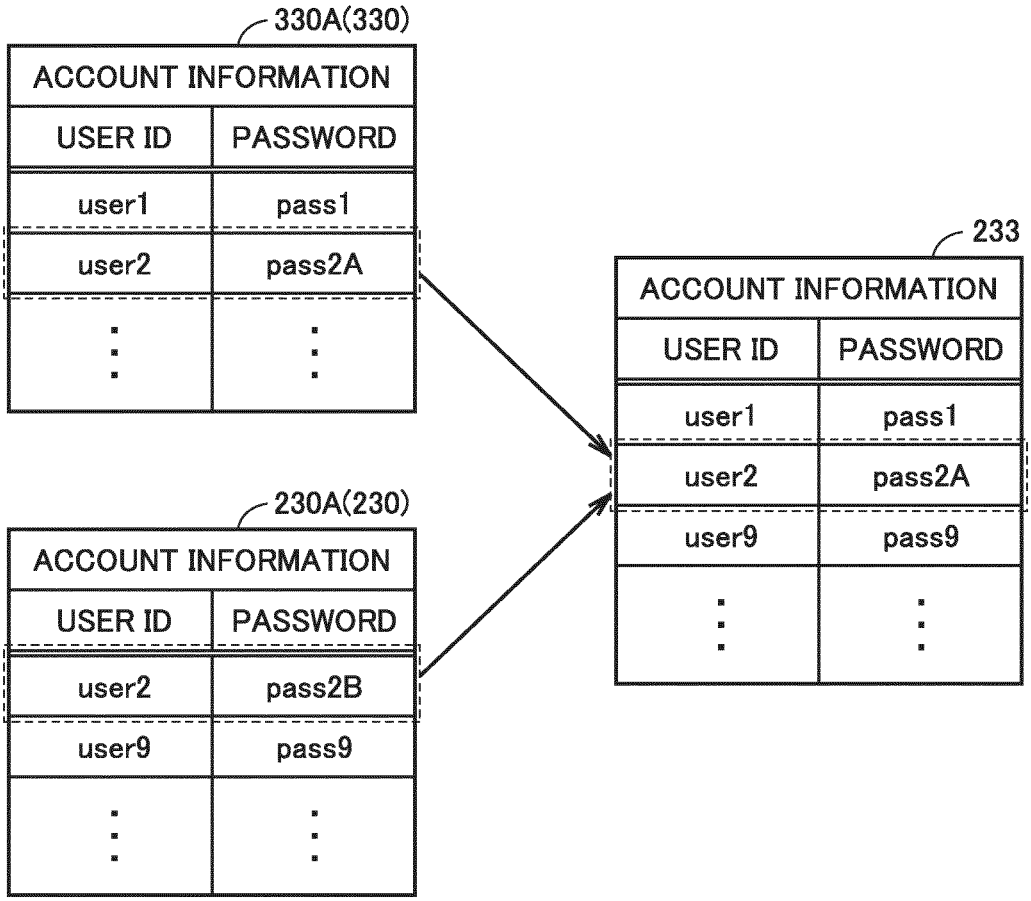

330A(330)
ACCOUNT INFORMATION
USER ID
PASSWORD
user1
pass1
user2
pass2A
230A(230)
ACCOUNT INFORMATION
USER ID
PASSWORD
user2
pass2B
user9
pass9
233
ACCOUNT INFORMATION
USER ID
PASSWORD
user1
pass1
user2
pass2A
user9
pass9

FIG.13

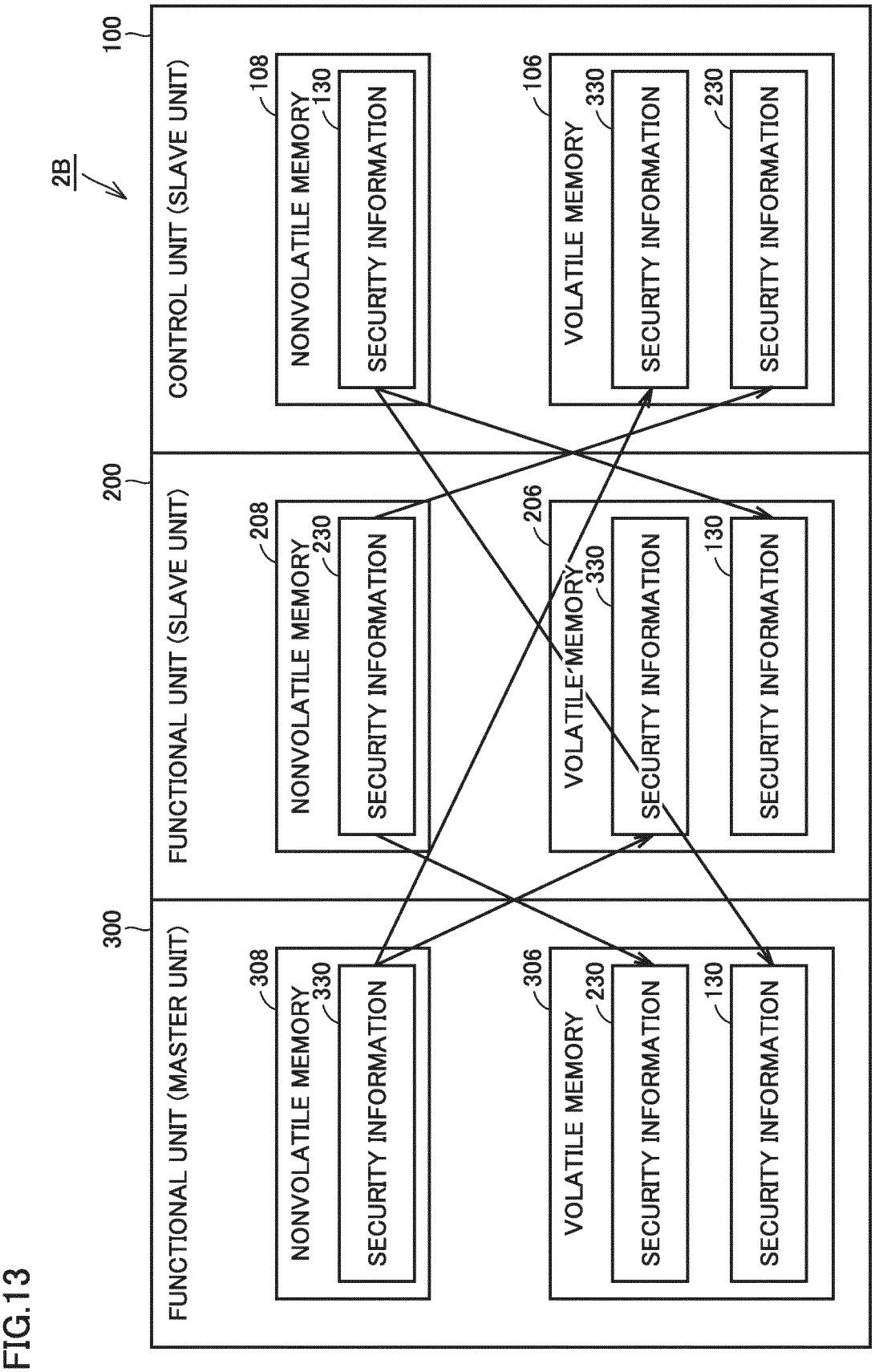

2B
100
CONTROL UNIT (SLAVE UNIT)
108
NONVOLATILE MEMORY
130
SECURITY INFORMATION
106
VOLATILE MEMORY
330
SECURITY INFORMATION
230
SECURITY INFORMATION
200
FUNCTIONAL UNIT (SLAVE UNIT)
208
NONVOLATILE MEMORY
230
SECURITY INFORMATION
206
VOLATILE MEMORY
330
SECURITY INFORMATION
130
SECURITY INFORMATION
300
FUNCTIONAL UNIT (MASTER UNIT)
308
NONVOLATILE MEMORY
330
SECURITY INFORMATION
306
VOLATILE MEMORY
230
SECURITY INFORMATION
130
SECURITY INFORMATION

FIG.14

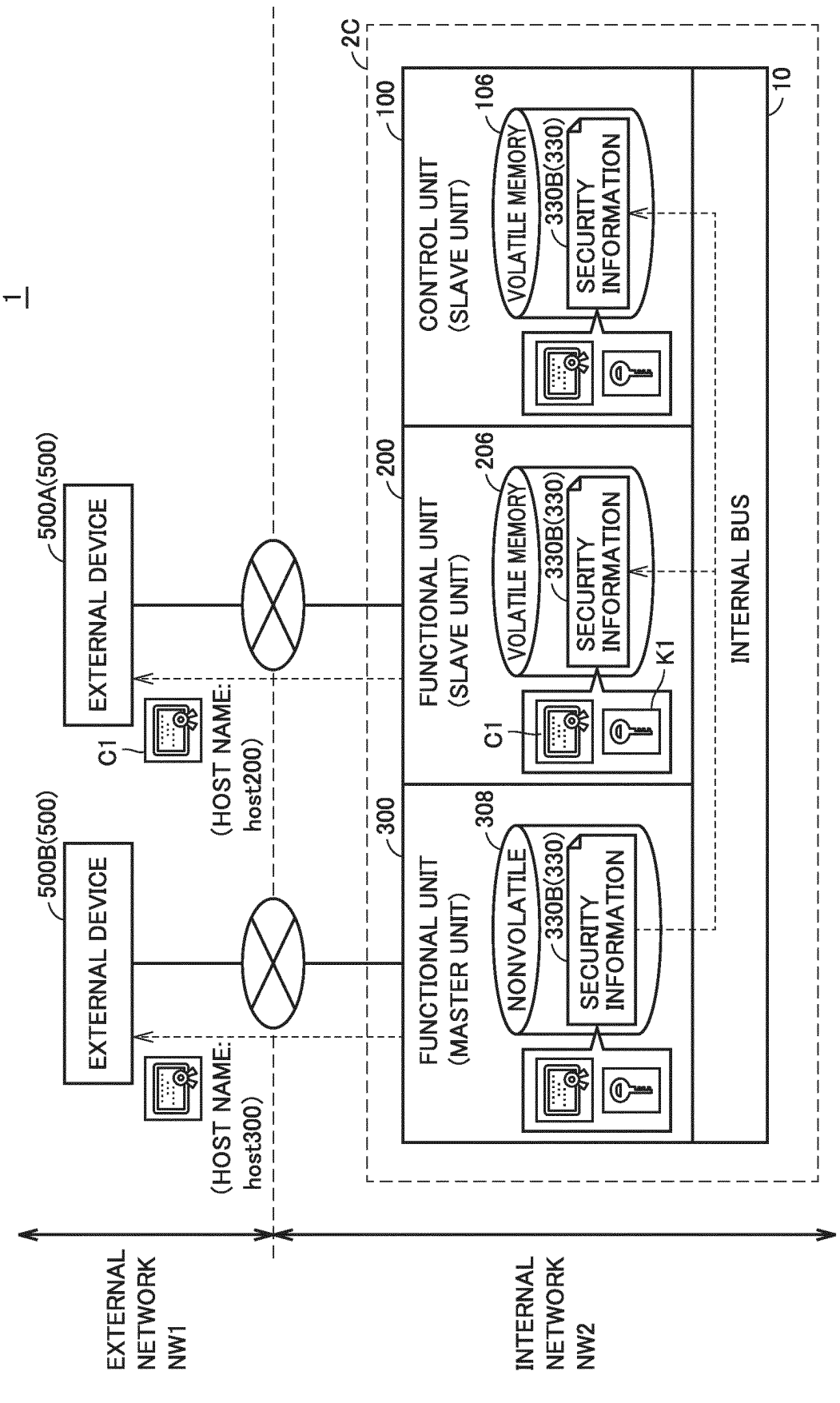
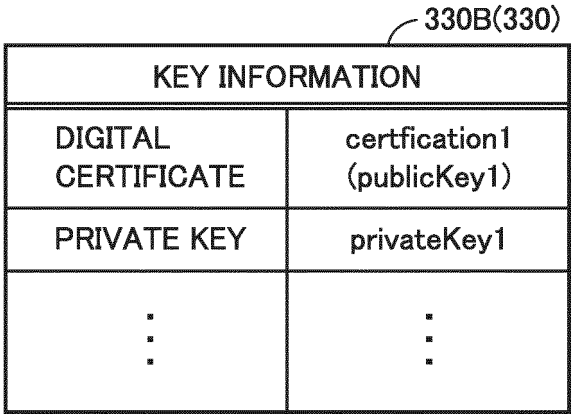

1
2C
10
100
200
300
CONTROL UNIT
(SLAVE UNIT)
FUNCTIONAL UNIT
(SLAVE UNIT)
FUNCTIONAL UNIT
(MASTER UNIT)
INTERNAL BUS
106
206
308
VOLATILE MEMORY
NONVOLATILE
330B(330)
SECURITY
INFORMATION
K1
C1
500A(500)
500B(500)
EXTERNAL DEVICE
(HOST NAME:
host200)
(HOST NAME:
host300)
EXTERNAL
NETWORK
NW1
INTERNAL
NETWORK
NW2

FIG.15


330B(330)
KEY INFORMATION
DIGITAL CERTIFICATE
certfication1 (publicKey1)
PRIVATE KEY
privateKey1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/009376

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/31(2013.01)i, G06F21/44(2013.01)i, G06F21/45(2013.01)i, G06F21/60(2013.01)i, H04L12/28(2006.01)i
FI: G06F21/31, H04L12/28200Z, G06F21/45, G06F21/44350, G06F21/60360
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int.Cl. G06F21/31, G06F21/44, G06F21/45, G06F21/60, H04L12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2020
Registered utility model specifications of Japan 1996-2020
Published registered utility model applications of Japan 1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2018-128722 A (HITACHI INDUSTRIAL EQUIPMENT SYSTEMS CO., LTD.) 16.08.2018 (2018-08-16), paragraphs [0013]-[0043]	1-2, 7-8 3-6
Y	JP 2010-79354 A (KOYO ELECTRONICS IND CO., LTD.) 08.04.2010 (2010-04-08), paragraphs [0002], [0003], fig. 5	1-2, 7-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10.06.2020	23.06.2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/009376

JP 2018-128722 A	16.08.2018	(Family: none)	
JP 2010-79354 A	08.04.2010	(Family: none)	

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2016194808 A **[0002] [0003]**